estos
enables easy communication

Technical and Organisational Measures

No.	Category	Description
0	**Organisation**	
	How is the implementation of data protection organised?	An external data protection officer is appointed to perform the advisory and control functions under the GDPR.
	Please provide us with the name and contact details of your data protection officer.	Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 14, 93047 Regensburg, Germany Tel: +49 941 2986930 E-Mail: c.volkmer@projekt29.de
	In what way are employees trained in the implementation of the agreed technical and organisational measures that are used for this processing?	Regular data protection training for all employees Obligation of all employees to the data protection declaration
	Are the processing procedures documented with regard to the admissibility of data protection law?	Yes, the data streams are documented within the framework of the internal procedural directory and the permissibility of processing and use is proven in accordance with the GDPR.
1	**Confidentiality (Art. 32 Abs. 1 lit. b GDPR)**	
1.1	**Physical Access Control**	
	How are the buildings in which the processing takes place protected against unauthorised access?	Alarm system in building part of the company.
	How are the rooms / offices in which the processing takes place protected against unauthorised access?	Fuse circuits of the alarm system. Access only for employees via dedicated RFID chip. Notification of security service and certain employees in case of alarm.
	How are the processing systems protected against unauthorised access?	Separate security circuit of the alarm system with access only for administrative personnel.
	How are the implemented access control measures checked for suitability?	Access control measures are also checked by the external data protection officer as part of the controls.
1.2	**Internal Access Control**	

No.	Category	Description
	How are user accesses assigned?	The department heads or managing directors report the entry of new employees to the administration. Employees receive Microsoft Active Directory (AD) accounts upon entry; authorizations are controlled via AD groups. (department, team or individually based affiliates)
	How is the validity of user accesses checked?	The department heads or managing directors are obliged to notify the administration in good time of any relevant changes in employment relationships.
	How are user accesses including application, approval procedures, etc. documented?	Requests for user access can only be requested or approved by department heads or managing directors by e-mail and are confirmed by the administration by e-mail. The progress is recorded via mail archiving.
	How is it ensured that the number of administration accesses is exclusively reduced to the necessary number and that only professionally and personally suitable personnel are employed for this?	Administration access is only granted to dedicated system administrators and substitutes on approval by the management. All relevant and eligible persons have a proven technical IT background with experience in administration. They are neither temporary nor employed as external employees, are not on probationary periods, and are bound by the company's privacy policy.
	Is access to the systems / applications possible from outside the company (home offices, service providers, etc.) and how is access structured?	Access is possible via an encrypted VPN connection (L2TP) for explicitly authorized employees. Identification is performed via the Microsoft Active Directory logon data and a pre-shared key.
1.3	**Electronic Access Control**	
	How is it achieved that passwords are known only to the respective user?	There are no shared user accounts. The users receive an individual initial password. A change of the password is technically enforced at the first login. The employees are instructed to handle passwords carefully and not to make them accessible to other persons.
	What are the requirements for the complexity of passwords?	Only passwords that are not part of the user logon or name, contain 3 out of 4 different character classes, and are at least 8 characters long are accepted.

No.	Category	Description
	How is it ensured that the user can / must change his password regularly?	Group policies (Microsoft Active Directory system settings) force a password change or block access after 60 days. The new password must not correspond to one of the three previous passwords.
	What organizational precautions are taken to prevent unauthorized access to personal data at the workplace?	Access authorisations are user- and group-based for the persons entrusted with processing. The systems are password protected. Work stations are automatically locked when inactive. Employees are instructed not to leave any visible or freely accessible personal data when leaving the workplace.
	How is it ensured that access authorizations are assigned according to requirements and for a limited period of time?	The management regularly checks the rights and user structure.
	How are access authorizations documented?	Via the access control lists in the systems.
	How is it ensured that access authorizations are not misused?	Sporadic review of the system protocols by the management.
	How long are protocols kept? Who has access to the logs and how often are they evaluated?	No fixed deadlines, usually system parameters, exclusively the management.
1.4	**Isolation Control**	
	How is it ensured that data collected for different purposes is processed separately?	A dedicated rights system is used to separate the data.
1.5	**Pseudonymisation**	
	What organizational measures have been taken to ensure that the processing of personal data complies with the law?	Regular data protection training for all employees Obligation of all employees to the data protection declaration
	How is personal data processed/stored so that it cannot be assigned to the persons concerned?	In most cases, the processing of personal data can be assigned to a data subject.
2	**Integrity (Article 32 Paragraph 1 Point b GDPR)**	
2.1	**Data Transfer Control**	

No.	Category	Description
	How do you ensure integrity and confidentiality in the transfer of personal data?	The data is passed on via encrypted channels and/or the encryption of the data itself. Access data will only be delivered or disclosed to the intended recipient.
	Are encryption systems used for the transfer of personal data and if so, which?	The data is sent by e-mail or made available via the Internet via server with transport encryption (TLS). Data is encrypted on a data medium basis using Microsoft BitLocker and/or encrypted ZIP archives (AES-256).
	How is the transfer of personal data documented?	n/a
	How is the unauthorized leakage of personal data limited by technical measures?	A strict assignment of rights protects the data from unauthorized access.
	Is there a control system that can detect an unauthorized leakage of personal data?	This is also checked as part of the checks under item 1.3.
2.2.	**Data Entry Control**	
	What measures are taken to track who accessed applications, when and for how long?	Access logs of servers and systems.
	How can it be traced which activities were carried out on the corresponding applications?	Access logs of the applications.
	What measures are taken to ensure that processing by the employees can only be carried out in accordance with the instructions of the client?	Training and sensitisation of employees through regular events and staff interviews.
	Which measures are taken to ensure that subcontractors also exclusively carry out personal data of the client to the agreed extent?	The data processing of subcontractors is carried out with clear order definitions and a formalised order placement.
	How is the deletion / blocking of personal data ensured at the end of the retention period for subcontractors?	Determined by contractual obligation, if the purpose no longer applies, deletion of the data is also indicated.

No.	Category	Description
3	**Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)**	
3.1.	**Availability Control**	
	How is it ensured that the data carriers are protected against elementary influences (fire, water, electromagnetic radiation, etc.)?	The backup data carriers are stored in an appropriate safe. Backup records are outsourced by the management on a regular basis.
	What protection measures are used to protect against malware and how is their actuality guaranteed?	Operating system security updates and anti-virus software and definitions are rolled out and updated centrally and automatically. Anti-virus and firewall solutions are used on client and server systems. Incoming mails are checked by the mail transport server for malware and falsified sending data before they are delivered.
	How is it ensured that data carriers that are no longer needed or are defective are properly disposed of?	The data carriers are disposed of centrally by the IT department. Functioning data carriers are securely deleted according to suitable methods. (e.g. multiple overwriting) Non-functional data carriers are physically destroyed.
3.2.	**Rapid Recovery**	
	Which organisational and technical measures are taken to ensure the availability of data and systems as quickly as possible in the event of damage? (rapid recoverability according to Art. 32 para. 1 lit.c GDPR)	The server and power supply systems of the processing plant are designed redundantly to prevent a failure.
4.	**Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)**	
	What procedures exist for regular evaluation/review in order to guarantee the security of data processing (data protection management)?	The external data protection officer regularly and in part unannounced checks compliance with the technical-organizational measures.

No.	Category	Description
	How do you react to inquiries and problems (Incident-Response-Management)?	Use of a ticket system (kayako) two-stage (1st and 2nd level); in addition telephone hotline and automated monitoring and alarming
	What data protection-friendly default settings are there (Art. 25 para. 2 GDPR)?	No pre-assignment by check marks; no pre-assignments are made when logging on to the system; the user must enter the logon information in each case
4.1	**Order or Contract Control**	
	What procedures are there for the instruction or handling of order data processing (data protection management)?	The contracts were prepared in accordance with the new guidelines for order data processing. The external data protection officer performs the corresponding advisory and control duties

Legal Information / Imprint

The information contained in this document reflects the state of knowledge at the time the document was created. Errors and subsequent alterations are reserved.

estos GmbH rejects any liability for damage caused by the direct or indirect use of this document. All brand and product names quoted are trademarks or property of their respective owners.

estos GmbH, Petersbrunner Str. 3a, 82319 Starnberg, Germany

info@estos.de
www.estos.de